מבצעי השפעה בסייבר ברשת האפלה (Dark Web)

לב טופור ופנינה שוקר

בשנים האחרונות חלה עלייה משמעותית בהיקפה ובעוצמתה של מלחמת המידע בין המעצמות והכוחות השונים בזירה הבין־לאומית, ומבצעי השפעה הפכו לכלי לגיטימי בידי שחקנים פוליטיים תועלתניים ומעצמות גלובליות כאחד. העיסוק העיקרי בהקשר זה הוא במִבצעי השפעה ברשתות החברתיות, והספרות המקצועית אינה מתייחסת באותה מידה למִבצעי השפעה הנעשים ברשת האפלה; עיקר העיסוק המחקרי במבצעים כאלה כיום הוא בהקשר של עשייה פלילית. הרשת האפלה פותחה על ידי הצי האמריקאי לצורכי מודיעין, ולאחר מכן קודמה על ידי המערב ככלי ציבורי להגנה על פרטיות ואנונימיות. כיום היא משמשת כר פורה להדלפות מכוונות של מדינות שאינן רוצות לפרסם מידע מסוים בכלי התקשורת המסורתיים. הדלפות אלו נתפסות כאותנטיות, מה שמוביל לעיתים את אמצעי התקשורת וארגוני מודיעין לבלוע את הפיתיון ולבחון את הדברים לעומקם, ובמקרים אחדים אפילו לשנות דפוסי פעולה. משרתו של מאמר זה היא להציג את האופן שבו נעשה שימוש ברשת האפלה לטובת מבצעי השפעה, בעיקר באמצעות הדלפה מכוונת של מידע.

מילות מפתח: רשת אפלה, מבצעי השפעה, תעמולה, לוחמת מידע, דיסאינפורמציה

מבוא

בינואר 2019 דלפו לרשת האפלה עשרות אלפי מסמכים ותכתובות דואר אלקטרוני של בכירי ממשל רוסיים, אנשי דת מהכנסייה האורתודוכסית הרוסית ואוליגרכים רוסיים. המידע הודלף, ככל הנראה, בעקבות פריצה ופעילות מכוונת של האקרים אקטיביסטים ("האקטיביסטים"), שהצהירו כי פעולות אלו נבעו לא ממטרה

לב טופור הוא יועץ אסטרטגי בכיר וחוקר גזענות וסייבר. פנינה שוקר היא חוקרת (מלגאית ניובאואר) במכון למחקרי ביטחון לאומי.

אידיאולוגית, אלא מהרצון להבטיח את חופש המידע: "אין לנו כל מטרה מלבד להבטיח כי המידע יהיה נגיש לטובת מי שזקוק לו יותר מכל – העם".[1] אירוע זה מלמד על השימוש שנעשה ברשת האפלה לעקיפת מגבלות שמשטרים טוטליטאריים מטילים על חופש הביטוי. אלא שבנוסף לכך, בשנים האחרונות ניכר ששחקנים רבים במערכת הבין־לאומית עושים שימוש בהדלפות מכוונות, בחלקן כוזבות, כדי ליצור השפעה פוליטית. כך מתחדד פעם נוספת המתח המובנה ברשתות האינטרנט בין הגנה על הפרטיות ובין צורכי הביטחון הלאומי.

באופן מסורתי, הרשת האפלה מהווה כר נרחב לפעילות פלילית, כמו גם להדלפות ולסחר במידע. בשנים האחרונות חלה עלייה משמעותית בהיקפה ובעוצמתה של מלחמת המידע בין השחקנים השונים בזירה הבין־לאומית באמצעות הרשת האפלה, כאשר כל צד משתמש בהדלפות מכוונות ובדיסאינפורמציה כדי לטפל את תודעת הצד השני. זאת, בין אם מדובר בהדלפה שמטרתה היא צבאית גרידא, ובין אם מדובר בהדלפה שמטרתה היא השפעה חברתית־אזרחית או אפילו עיסקית. לדוגמה, מדינות שאינן מעוניינות לפרסם דברים מסוימים בצורה רגילה בתקשורת המסורתית מדליפות מידע ברשת האפלה, תוך ניסיון לשוות למידע מראית עין של אותנטיות. בנוסף לכך, כלי התקשורת עצמם הקימו פלטפורמות שמטרתן לספק יכולת תקשורת מוצפנת שנועדה לעודד הדלפות. כאלו הן פלטפורמות דוגמת WikiLeaks ו־Secure Drop, עליהן יבוא פירוט בהמשך המאמר. כמו כן, ברשת האפלה מוצעות למכירה נוזקות, רוגלות, תולעים ועוד אין ספור תוכנות וקבצים זדוניים, וכן כלי הצפנת תקשורת וסייבר אחרים (למשל, מדריכי הצפנת PGP והצפנות אחרות קלות לשימוש).

מטרתו של מאמר זה היא להציג את האופן שבו שחקנים בזירה הבין־לאומית עושים שימוש ברשת האפלה כדי להפיץ תעמולה ודיסאינפורמציה נגד יריבים, וכיצד פעולות אלו עשויות להיתרגם למבצעי השפעה רחבי היקף. המאמר בנוי משלושה חלקים: החלק הראשון כולל סקירה תיאורטית העוסקת במניפולציה של מידע בכלל ובמבצעי השפעה בפרט, תוך הבאת מספר דוגמאות למבצעי השפעה מרכזיים בשנים האחרונות; החלק השני עוסק ברשת האפלה, מאפייניה ושימושיה העיקריים; בחלק השלישי, המשלב את שני החלקים הראשונים, מוצגים האופן שבו נעשה שימוש ברשת האפלה כדי להוציא לפועל מבצעי השפעה, ולצד זאת היקפה של התופעה.

1 Stephan Jajecznyk, "The Dark Side of the Kremlin: Hacked Russian Documents Explained", *Al Jazeera*, February 25, 2019.

מהם מבצעי השפעה?

מִבצע השפעה הוא יישום מתואם, משולב ומסונכרן של יכולות דיפלומטיות, אינפורמטיביות, צבאיות וכלכליות, כמו גם יכולות לאומיות אחרות, וזאת בעיתות שלום, בזמני משבר, במצבי עימות ובמצבים שלאחר עימות. המטרה של מבצע ההשפעה היא להשפיע על התנהגויות או החלטות של קהלי יעד זרים, כך שיאמצו עמדות ההולמות את האינטרסים של יוזמי המבצע.[2]

מבצעי השפעה על התודעה הם דפוס פעולה מוכר, אשר נועד לשרת מגוון תכליות מדיניות, ביטחוניות, כלכליות וחברתיות. מבצעי השפעה על התודעה ברמה המדינית נועדו להשיג את יעדיהם באמצעות, בין היתר, פגיעה בביטחון האישי והכלכלי, ערעור האמון והתמיכה של הציבור במוסדות המדינה ופגיעה בלכידות החברתית. האמצעים להשגת תכליות אלו כוללים התערבות פעילה במערכות ובתהליכים, או הפעלת מנופים שונים כדי להניע לפעולה או להניא מפעולה, השגת מידע ושימוש בו ליצירת מסרים, הפצה של מסרים ויצירת תהודה להשגת אפקט מרבי. הערוצים להעברת המסרים הם המדיה המסורתית, ולצידה המדיה החדשה, דהיינו האינטרנט והרשתות החברתיות המתנהלות על גביו. מובילי דעה משמשים לעיתים כ"סוכנים לא מודעים" לחיזוק אמינותם של המסרים ולהגברת תפוצתם.[3]

בשנים האחרונות גוברים ניסיונות של גורמים זרים (מדינות וגורמים לא מדינתיים) להתערב במערכות בחירות של מדינות יריבות באמצעות כלים דיגיטליים. פעילות זו נעשית בחלקה באמצעות תקיפות סייבר על מערכות המחשוב התומכות את תהליך הבחירות באותן מדינות (מסדי נתונים, תוכנות למיניהן ומערכות תקשורת) במטרה לשבש את הנתונים, לגנוב אותם כדי לעשות בהם שימוש, או לפגוע ביכולת הפעולה של מערכות אלו. לצד פעילות זו, נעשים מאמצים רחבי היקף להטיית השיח באותן מדינות, שמטרתם היא להשפיע על תודעת הבוחרים.

הסוג השלישי של מבצעי תודעה מהווה סינתזה של השניים הראשונים: מבצעי השפעה על התודעה באמצעות שימוש בסייבר. המטרות של ניסיונות אלה עשויות להיות מגוונות: החל מניסיון לערער את אמון הציבור בתהליך הדמוקרטי וכלה בניסיון להשפיע על התמיכה במפלגות ובמועמדים שונים. חלק מהניסיונות

---

2 Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, Cathryn Quantic Thurston, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (California: RAND Corporation, 2009), p. 2.

3 רון שלייפר, "הלוחמה הפסיכולוגית בעופרת יצוקה", **מערכות**, 432, אוגוסט 2010, עמ' 19–20.

אף נועד להניא אנשים מלהשתתף בבחירות, וזאת על בסיס זהותם או מעמדם הסוציו־אקונומי.[4]

השחקנים העיקריים המוציאים לפועל ניסיונות מהסוגים שנמנו לעיל הם משטרים אוטוריטריים, דוגמת רוסיה, סין ואיראן. גם משטרים דמוקרטיים־ליברליים, דוגמת ארצות הברית, בריטניה ואף ישראל, מנסים להשפיע בדרכים כאלו בזירה הבין־לאומית. למשל, לרוסיה יש מסורת ארוכה של פעולה בתחום מבצעי ההשפעה והיא מחזיקה במשנה סדורה וביכולות מבצעיות לשם כך.[5] על שיטות הפעולה הרוסיות בתחום מבצעי ההשפעה ניתן למנות הפצת ידיעות כוזבות ברשתות החברתיות על ידי פרופילים מזויפים; רכישת פרופילים אותנטיים במטרה להפיץ פרסומות פוליטיות שתומכות במועמדים פרו־רוסיים במערכות בחירות ברחבי העולם וכדי לפרסם ידיעות כוזבות או מידע מפליל על יריבי מוסקבה; שימוש נרחב בתקשורת הממוסדת הרוסית הנמצאת בבעלות הקרמלין במטרה להפיץ מידע כוזב ומניפולטיבי.[6] כך, במחצית השנה האחרונה בלבד הוצאו לפועל מבצעי השפעה רוסיים סביב מערכות בחירות רבות ברחבי העולם, בכללן הבחירות הכלליות בספרד, הבחירות לפרלמנט האירופי, הבחירות האחרונות בניגריה, אינדונזיה, דרום אפריקה ועוד.[7]

גם סין עושה שימוש ענֵף בתעמולה ובמבצעי השפעה, הן בכדי לעצב את תדמיתה של המפלגה הקומוניסטית הסינית והן בכדי לערער את יציבותן של יריבותיה.[8] לאחרונה הולכים ורבים הדיווחים על מאמציה של סין להתערב בבחירות במדינות רבות, דוגמת סרי לנקה, מלזיה ואוסטרליה.[9] בנוסף לכך, ערב בחירות אמצע הכהונה בארצות הברית הודיע הממשל האמריקאי כי סין, יחד עם איראן

---

4 Chris Tenove, Joran Buffie, Spencer McKay and David Moscrop, *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy* (The University of British Columbia: Center for the Study of Democratic Institutions, 2018), p. 26.

5 דימה אדמסקי, "אומנות אופרטיבית קיברנטית: מבט מזווית לימודי האסטרטגיה ומפרספקטיבה השוואתית", **עשתונות** 11, מרכז המחקר, המכללה לביטחון לאומי, 2015, פרק ב': "הגישה הרוסית לאומנות המערכה הקיברנטית", עמ' 28–48.

6 Alina Polyakova, "Want to Know What's Next in Russian Election Interference? Pay Attention to Ukraine's Elections", *Brookings*, March 28, 2019; Michael Schwirtz and Sheera Frenkel, "In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering", *The New York Times*, March 29, 2019.

7 פנינה שוקר, "התערבות זרה בבחירות בעולם: מאפיינים, מגמות ולקחים לישראל", **מבט על**, מס' 1173, 10 ביוני 2019.

8 Erica Pandey, "How China Became a Global Power of Espionage", *AXIOS*, March 23, 2018.

9 Prashanth Parameswaran. "China's Influence Operations in Asia: Minding the Open Door Challenge", *The Diplomat*, May 14, 2019.

ורוסיה, מנסות לערער את ההליך הדמוקרטי באמצעות קמפיין תעמולתי מקוון, שכולל הפצת דיסאינפורמציה ברשתות החברתיות במטרה להעמיק את השסעים האידיאולוגיים בארצות הברית וללבות ויכוחים פנימיים בסוגיות שעל סדר היום המקומי.[10] במסגרת יריבותה עם ארצות הברית, סין מנסה גם לקדם את השפעתה בסינגפור: לאחרונה פורסם כי המפלגה הקומוניסטית הסינית פונה אל סינגפורים ממוצא סיני, בעיקר באמצעות אפליקציית Wechat הסינית, לצורך השפעה על הפוליטיקה והחברה בסינגפור.[11] במקביל דווח כי נחשף מאמץ השפעה סיני בהיקף חסר תקדים על גבי פלטפורמות "פייסבוק", "טוויטר" ו"יוטיוב" – שלושתן אסורות בשימוש בסין עצמה – כדי להנמיך את גובה הלהבות במחאות הסוערות בהונג קונג נגד מעורבותה של סין בנעשה במקום.[12]

גם אירן אינה טומנת ידה בצלחת; באוגוסט 2018 מחקו "טוויטר" ו"פייסבוק" מאות חשבונות החשודים כמקושרים למבצע דיסאינפורמציה אירני.[13] התוכן שהועלה בחשבונות אלה נועד להבליט נושאים ונרטיבים ההולמים את מדיניות החוץ האירנית ולקדם נושאים אנטי־סעודיים, אנטי־ישראליים ופרו־פלסטיניים, וכן לעורר תמיכה בנושאים מסוימים במדיניות ארצות הברית המשרתים את האינטרסים האירניים, כמו הסכם הגרעין בין אירן ובין המעצמות מ־2015.[14] בשלהי אוקטובר 2018 גם נחשפה רשת עמודי "פייסבוק" שמקורה באירן, שנועדה להשפיע על דעת הקהל בארצות הברית ובבריטניה.[15] כמו כן, לאחרונה הולכים ורבים הדיווחים על תקיפות סייבר ומבצעי השפעה איראניים נגד ישראל. בסוף ינואר 2019 הצהיר ראש הממשלה נתניהו בכנס Cyber Tech כי אירן מנסה להשפיע על הבחירות בישראל דרך חשבונות מזויפים ברשת, וכי היא מבצעת מתקפות סייבר נגד ישראל "על בסיס יומי".[16] בניגוד למאמצי ההשפעה הרוסיים

---

10 Abigail Grace, "China's Influence Operations Are Pinpointing America's Weaknesses", *Foreign Policy*, October 4, 2018.

11 Muhammad Faizal Bin Abdul Rahman, "Foreign Influence in Singapore: Old Threats in New Forms", *The Diplomat,* July 23, 2019.

12 Raymond Zhong, Steven Lee Myers and Jin Wu, "How China Unleashed Twitter Trolls to Discredit Hong Kong's Protesters", *The New York Times,* September 18, 2019.

13 Craig Timberg, Elizabeth Dwoskin, Tony Romm, Ellen Nakashima, "Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation", *The Washington Post*, August 21, 2018.

14 Adriane M. Tabatabai, "A Brief History of Iranian Fake News: How Disinformation Campaigns Shaped the Islamic Republic", *Foreign Affairs*, August 24, 2018.

15 "פייסבוק נלחמת בפייק ניוז מאירן: 'חיסלנו רשת תעמולה – מיליון משתמשים נחשפו'", **דה מרקר**, 27 באוקטובר 2010.

16 סתו נמר, "נתניהו: אירן מתקיפה את ישראל בסייבר על בסיס יומי", **מעריב**, 29 בינואר 2019.

המוּבָּרים המגלים רמת תחכום גבוהה יחסית, המאמצים האיראניים והמאמצים הסיניים ניחנו ברמת ביצוע ירודה למדי, וניתן להתחקות אחריהם בקלות יחסית.

מערכות בחירות שנערכו ברחבי העולם במחצית השנה האחרונה התקיימו בצל החשש ממבצעי השפעה. ואכן, ברבות מהן זוהו מאמצי השפעה, בעיקר רוסיים. מניתוח מאמצים אלה עולה כי פעולות נגד, שננקטו על ידי ענקיות המדיה והמדינות עצמן, הביאו להפחתת ניסיונות ההשפעה הזרה באמצעות בוטים שנעשו ברשתות החברתיות. לעומת זאת, ניתן לזהות כיום פעילות גוברת מצד סוכני השפעה אנושיים. זאת ועוד, מאמצי ההשפעה בתקשורת הממוסדת שבים למלא תפקיד משמעותי, וכמוהם גם מאמצי השפעה באפליקציות להעברת מסרים מיידיים, דוגמת "ווטסאפ" ו"טלגרם", להן מיוחסת רמת מהימנות גדולה יותר: המידע מועבר בפלטפורמות סגורות אלו בתוך קבוצות מצומצמות יחסית של חברים ומשפחה, מה שמעניק למסרים מראית עין של מהימנות. יתרה מזאת, טכנולוגיית ההצפנה מקצה לקצה, המאפיינת פלטפורמות אלו, אינה מאפשרת אפילו למנהליהן גישה למסרים שנשלחים בהן, אלא אם כן משתמש מדווח על תוכן מסוים כבעייתי. מאפיינים אלה מקשים על ניטור מידע כוזב והסרתו.[17]

הרשת האפלה: מאפיינים ושימושים

בשנים האחרונות הפכה הרשת האפלה לאחד הנושאים המדוברים ביותר בקרב העוסקים בביטחון סייבר.[18] כדי להבין כיצד נוצרה והתפתחה הרשת האפלה ומהם מאפייניה הייחודיים, יש להתחיל בסקירה קצרה של מאפייני הרשת הרגילה: רשת האינטרנט הרגילה (Surface Web) נוצרה מפרויקט תקשורת של משרד ההגנה של ארצות הברית בשנות השישים של המאה העשרים, הידוע בשם Advanced Research Project Agency Network – ARPANET. ב־1983 שונה הפרויקט מרשת סגורה (Network Control Protocol – NCP) לפרויקט פתוח, הידוע כיום בשם "פרוטוקול שליטה" או "פרוטוקול אינטרנט" /Transmission Control Protocol Internet Protocol – TCP/IP)).[19] פתיחת הרשת הביאה להרחבה מסיבית של רשת האינטרנט – ממספר חיבורים בודדים לכדי מיליונים כיום – ולחלוקה מעמדית של רשתות – רשת ארצית (National, Class A), רשת אזורית (Regional, Class B) ורשת מקומית (Local, Class C) – והניחה את התשתית לרשת האינטרנט

17 שוקר, "התערבות זרה בבחירות בעולם: מאפיינים, מגמות ולקחים לישראל".

18 Mihnea Mirea, Victoria Wang and Jeyong Jung, "The Not So Dark Side of The Darknet: A Qualitative Study", *Security Journal* 32 no. 2 (2019): 102-118.

19 George Hurlburt, "Shining Light on the Dark Web", *IEEE Computer* 50, no. 4 (2017): 100-105.

הציבורית המוכרת לנו כיום. רשת האינטרנט של ימינו היא רשת המחברת מספר מחשבים/מכונות דרך צמתים (Nodes) או נקודות גישה.[20]

פרויקט ARPANET נסגר רשמית ב־1989 והותיר אחריו את תחומי הרשת הציבוריים: כתובות מאגרי מידע (דפי אינטרנט) ופרוטוקולי רשת נגישים, דפדפנים לכלל הציבור ושפת רשת נגישה (למשל שפת HTML). לצורך הפיכת האינטרנט לנגיש לכלל הציבור, הוקם ארגון ICANN (Internet Corporation for Assigned Names and Numbers), אשר סיפק כתובות ומספרי רשת וצירף שמות לכתובות IP. הארגון החל למפתח כמעט כל שירות ומידע ציבורי והזמין חברות טכנולוגיות רבות לבנות מאגרי מידע נגישים לציבור, דוגמת Google, Bing, AOL, Yandex.ru ועוד.[21] התוצאה הייתה שחברות ענק וממשלות יכלו לעצב את רשימות החיפושים כראות עיניהן, ובדרך זאת לשלוט במידע הנגיש לציבור ולמנוע ממנו צריכת מידע שלא רצוי להן. כך נוצרה למעשה הרשת העמוקה.[22]

הרשת העמוקה היא כל סוג של מידע שאינו ממופה על ידי מנועי חיפוש והגישה אליו מוגבלת, אך נעשית באמצעות דפדפנים (תשתיות) רגילים; למשל, דפי אינטרנט דינמיים, דפי אינטרנט ללא קישורים, דפי אינטרנט שאינם מבוססים על Hyper Text Markup Language (HTML) ומאגרי מידע מוגבלים אחרים. גורמי ביטחון רבים מקיימים גם רשתות פרטיות (למשל, מקומיות) וכן רשתות עמוקות, כמו למשל רשת צבאית או רשת משטרתית, שהציבור הרחב לא יכול לגשת אליהן. יחד עם זאת, הרשת העמוקה מורכבת גם ממידע פרטי, דוגמת מאגרים פיננסיים, מאגרי מידע ביומטרי, רפואי וכדומה. לדוגמה, כאשר משתמש נכנס לחשבון הבנק שלו, הוא נכנס לרשת העמוקה, אך כאשר הוא נמצא בדף הבית של הבנק שלו, הוא נמצא ברשת הרגילה.[23]

הרשת האפלה (Darknet/Dark web) מהווה חלק מהרשת העמוקה, ולמעשה היא השכבה החבויה ביותר בה.[24] ניתן לגלוש אליה רק באמצעות דפדפן מיוחד או הגדרת פרוטוקולי רשת מיוחדים, כך שהפעולות הנעשות בה הן ברוב המקרים

---

20 Mitch Waldrop, *DARPA and the Internet Revolution: 50 Years of Bridging the Gap* (Defense Advanced Research Projects Agency, 2018).

21 Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, and Martin Rösler, "The Deep Web", *Trend Micro*, 2015.

22 Lucas D. Introna and Hellen Nissenbaum, "Shaping the Web: Why the Politics Search Engines Matters", *The Information Society* 16, no. 3 (2000):169-185; Eszter Hargittai, "The Social, Political, Economic and Cultural Dimensions of Search Engines: An introduction", *Journal of Computer-Mediated Communication* 12, no. 3 (2007): 769-777.

23 Hurlburt, "Shining Light on the Dark Web", pp. 100-105.

24 Gabriel Weimann, "Going Darker: The Challenge of Dark Net Terrorism", *Wilson Center*, April 27, 2018.

אנונימיות לחלוטין. המאפיינים הייחודיים של הרשת האפלה, לעומת הרשת העמוקה, הם הפרוטוקולים (הכללים) המיוחדים והתשתית המיוחדת הנדרשים לצורך שימוש וגלישה בה. התשתית המיוחדת מגיעה לעיתים בצורת דפדפנים המתוכנתים לגשת לפרוטוקולים שונים, כגון כתובות Onion, Riffle, Freenet או i2p ועוד, או בתור הגדרות רשת מסוימות הידועות רק לצדדים המשתמשים ברשת.[25] ארגונים ופרטים, למשל כוחות צבא, מודיעין ומשטרה, ואף ארגונים עיסקיים ופרטים בודדים, יכולים להקים רשתות אפלות, שהפרוטוקולים והדפדפנים שלהן יהיו מיוחדים וידועים רק למקימיהן.[26]

הרשת האפלה הנפוצה ביותר היא The Onion Route (TOR), אשר פותחה על ידי מעבדות הצי האמריקאי במטרה לאפשר תקשורת פרטית ואנונימית בקרב אנשי מודיעין ונחשפה בשנת 2002. רשת זו מורכבת מעשרות אלפי אתרי אינטרנט שאליהם ניתן לגשת רק באמצעות דפדפן TOR. אתרים אלה מכונים אתרי "בצל" על שם סיומת ה־onion המאפיינת אותם ודימוי הבצל, המשמש כמטאפורה לשכבות הרבות המקשות על הגישה למקור. אתרי הבצל אינם מקוטלגים, ואין מנוע חיפוש מרכזי היכול לסייע בצורה מסַפקת במציאתם. רשת TOR פועלת באופן שהתקשורת בין שתי נקודות (למשל, המחשב של המשתמש והאתר אליו הוא גולש) אינה מועברת בצורה ישירה, אלא דרך מספר תחנות ביניים (כתובות IP). כל תחנה מקבלת אמצעי ייחודי לפענוח, יודעת רק מהי התחנה הבאה בשרשרת ואינה יודעת מהי התחנה הסופית או מהו המקור. הסיבה לכך היא שחלק נכבד מהשרתים מוצפן, כך שספק האינטרנט יכול לגלות ברוב המקרים את הצומת הראשון אליו מגיע המשתמש, אך לא את הצמתים הבאים.[27] גם השרת המקבל את הקריאה לא יכול לאתר את הצמתים, אלא רק את הצומת שממנו הוא מקבל את הקריאה למידע/אינטראקציה. למעשה, גם צומת זה מוחלף מדי מספר דקות. בדרך זו, כל הצמתים הנמצאים באמצע הדרך מוגנים ברוב המקרים מפני מעקב פרטי או ממשלתי.[28]

הבעיה העיקרית ברשת TOR טמונה בייחודה: היא מאפשרת אבטחה ואנונימיות, אך היא אינה סמויה עבור ספקי רשת מקומיים. אלה אמנם אינם יכולים לגלות

25 Dakota S. Rudesill, James Caverlee and Daniel Sui, *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box*, Ohio State Public Law Working Paper No. 314 (Ohio State University, Woodrow Wilson International Center for Scholars, 2015).

26 Ibid; Lev Topor, "Deep and Dark Webs – Liberty or Abuse", *International Journal of Cyber Warfare and Terrorism* 9, no. 2 (2019): 1-14.

27 רועי גולדשמידט, "שימוש בתשתיות תקשורת אנונימיות על גבי הרשת למטרות פשיעה", *מרכז המחקר והמידע של הכנסת*, ינואר 2012.

28 Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing* (London: Global Commission on Internet Governance and Chatham House, 2015).

את המידע והיעדים של משתמשי הרשת, כמו למשל של פעילי מודיעין מערביים במדינות העוינות למערב, אך שימוש בדרך השלילה פתר בעיה זו, לפחות חלקית: ספקי רשת מקומיים יכולים לגלות שמתוך מספר משתמשים מסוים בשכונת מגורים, למשל, משתמש או מספר משתמשים בודדים היו בעלי תעבורת רשת יוצאת דופן. בדרך זו, כל מה שהממשל יכול היה לראות היה תעבורת רשת רגילה, וכל מה שהוא לא יכול היה לראות היה גלישה פרטית ואנונימית.[29]

פרט לתעבורת הרשת המיוחדת המאפיינת את הרשת האפלה, שכאמור עושה מסלול מבלבל וקשה לאיתור במספר צמתים, פלטפורמת TOR, המגיעה בצורת דפדפן נוח לשימוש, יכולה למנוע מאתרים לדלות מידע על משתמשים. הפרטיות היא דבר מקודש ברשת TOR, ואף אתר אינו יכול לדלות מתוכה מידע לגבי מיקום, סוגי חומרה, סוגי תוכנה ודפוסי פעילות. ניתן גם לבטל בדפדפן של TOR את השימוש ב־JavaScript, HTML 5, Media, Images, Icons, Symbols ועוד. כך יוצרת הרשת האפלה פרדוקס מעניין: מצד אחד, היא מקדשת את הפרטיות והאנונימיות, ומצד שני, דווקא יתרונות אלה הופכים לחסרונות כאשר נעשה בהם שימוש על ידי ארגוני פשיעה וטרור וגורמים עוינים, שכן הם מאפשרים להם לסחור במידע בחתימה נמוכה.[30]

בנוסף לנאמר לעיל, הרשת האפלה מהווה מעין שוק לביצוע פעולות לא חוקיות המאפשר, בין היתר, סחר בכלי סייבר. כך, למשל, אם חברה מסוימת מעוניינת לגרום נזק לחברה מתחרה, יש באפשרותה להיכנס לרשת האפלה, לקנות מתקפת כופר, נוזקה או רוגלה ולהפעיל רשת בוטים או כל כלי אחר. ברוב המקרים, הקונה והמוכר מבצעים העברה בביטקוין, מה שמאפשר את שמירת האנונימיות. רשתות אפלות משמשות אפילו כזירות למסחר בנשק ובסמים ולהפצת תכנים פורנוגרפיים,[31] ומהוות כר נוח לפעילות של ארגוני טרור: במשך כעשור, חלק ניכר מהתקשורת בין מנהיגי "אל־קאעידה" ברחבי העולם התנהל על גבי הרשת האפלה.[32] מן העבר השני, ברשת פועלים גופים שייעודם סיכול טרור, כמו למשל ארגוני ביטחון פנים ומודיעין.[33] לפי נתוני חברת Webhose, כחמישים אחוזים מהפעילות ברשת האפלה היא פלילית, שמשמעותם הנוספת היא שמחצית מהפעילות הינה חוקית ולגיטימית.

לאחרונה ניכרת עלייה בשימוש ברשת האפלה ככלי להתארגנות ומידע עבור פעילים במשטרים טוטליטאריים. ברשת האפלה יש גם אתרי מראה (Mirror)

29 Topor, "Deep and Dark Webs – Liberty or Abuse".
30 Ibid.
31 Nyshka Chandran, "From Drugs to Killers: Exploring the Deep Web", *CNBC,* June 23, 2015; Cara McGoogan, "Dark Web Browser Tor is overwhelmingly Used for Crime, Says Study", *The Telegraph,* February 2, 2016.
32 Weimann, "Going Darker".
33 Topor, "Deep and Dark Webs – Liberty or Abuse".

לאתרים מוכרים, כמו אתרי חדשות מערביים ומידע, כדי שאנשים החיים במשטרים טוטליטאריים יוכלו להגיע אליהם. כך, למשל, הכתובת facebookcorewwwi.onion מובילה ל"גרסת הבצל" של הרשת החברתית עבור משתמשים במדינות שבהן רשת "פייסבוק" חסומה. באופן דומה, הכתובת nytimes3xbfgragh.onion מובילה ל"גרסת הבצל" של "ניו יורק טיימס". בנובמבר 2018 העלה מהנדס לשעבר בחברת "פייסבוק" "גרסת בצל" ל"ויקיפדיה" – גרסת מראה ברשת האפלה לאנציקלופדיה החופשית, שחסומה לחלוטין או באופן חלקי במדינות שונות.[34] בעוד משטרים טוטליטאריים מתמודדים עם בעיית האנונימיות באמצעות מעצרים וחקירות, הממשל האמריקאי בחר להציף את העולם ברשת TOR, תוך קריאה לקידום חופש הביטוי וזכויות אדם, אנונימיות, תקשורת חופשית ופתוחה והתנגדות למשטרים טוטליטאריים.

שימושים פוטנציאליים ברשת האפלה למִבצעי השפעה

בעבר, כאשר מעצמה רצתה להשפיע על שחקן אחר בזירה העולמית – מדינה, ארגון טרור או אדם מסוים – היא עשתה שימוש בעוצמה צבאית או כלכלית. העידן הקיברנטי הוסיף ממד חדש למושג "עוצמה", בשלבו יכולות קיברנטיות מתקדמות וקלות לתפעול, שיש בהן כדי להפוך את יחסי הכוחות על פניהם ולעיתים אף להוות "שוברות שוויון". לדוגמה, מדינה יכולה לפתח פרויקט צבאי סודי, שעשוי לרדת לטמיון אם פושעי סייבר ומדליפים אחרים יחשפו אותו ברשת.[35] כך, למשל, ביולי 2018 נחשף כי האקר אמריקאי ניסה למכור ברשת האפלה תוכניות רגישות של מל"ט צבאי בשם MQ-9;[36] חברה מתחום התעשייה הצבאית פנתה במהלך השליש השני של שנת 2019 לאחד מכותבי מאמר זה וביקשה לאתר הדלפות עליה ברשת האפלה משום שחששה מפני הדלפת תוכניות רגישות שלה על ידי מספר עובדים מתוכה.

להלן יוצגו מספר פלטפורמות ברשת האפלה העשויות לשמש למבצעי השפעה: 1. פלטפורמות הדלפה; 2. פלטפורמות פסיביות שייעודן אחסון מידע; 3. פלטפורמות סחר. אלו כוללת הצעות למכירת מידע, כלי סייבר התקפיים ובוטים, ואף הצעות ל"מעורבות" מזויפת ברשתות החברתיות.

---

34 אמיתי זיו, "הצד האפל של האינטרנט: סמים, נשק, מתקפות סייבר ומתנגדי המשטר", **דה מרקר**, 18 ביולי 2018.

35 Joseph S. Nye. "Soft Power and American Foreign Policy", *Political Science Quarterly* 119 no. 2 (2004): 255-270; Ernest J. Wilson, "Hard Power, Soft Power, Smart Power", *The Annals of the American Academy of Political and Social Science* 616 no. 1 (2008): 110-124.

36 זיו, "הצד האפל של האינטרנט: סמים, נשק, מתקפות סייבר ומתנגדי המשטר".

פלטפורמות הדלפה

בעידן בו ניתן לגנוב יותר מטָרה־בייט אחד של מידע בשבריר שנייה באמצעות החסן נייד ולהדליף באופן אנונימי בזמן אמת מידע מישיבות ממשלתיות, ביטחוניות ועיסקיות, אין זה מפתיע שתדירותן של ההדלפות גברה.[37] הדלפות משמשות פעמים רבות את אלה המתנגדים לפעולות שנויות במחלוקת, בעיקר בנושאים הקשורים לצבא ולביטחון. יחד עם זאת, לא מעט פעמים הממשל המקומי הוא זה שמפעיל מדליפים, הן באמצעות הפעלה ישירה והן באמצעות הפעלה משוטה: כפי שארגוני ביטחון ושיטור מפעילים סוכנים הפועלים ברשת האפלה (והרגילה) או מתחזים לקטינים כדי ללכוד פדופילים, כך ארגוני מודיעין בכל העולם מפעילים פלטפורמות הדלפה, מפיצים מעין "קולות קוראים" להדלפות ומציעים תשלום עבורן. יתרה מכך, ממשלות רבות אף פונות לספקים חיצוניים, כגון חברות מודיעין עיסקי או חברות היי־טק, כדי לנטר, לנתח ולהפעיל גורמים מסוימים ברשת האפלה.[38] חשוב לציין בהקשר זה שפרויקט הרשת האפלה עלול להיות מלכודת דבש גדולה.[39]

דוגמה מובהקת נוספת לפלטפורמת הדלפה היא אתר העיתונות החופשית "ויקיליקס", שהוקם ב־2006 והספיק מאז לעורר מספר מהומות תקשורתיות לאחר שהדליף מאות אלפי מסמכים, ידיעות וחומרים נוספים על פעילות אמריקאית שנויה במחלוקת. האתר נמצא ברשת האינטרנט הרגילה, אך ממליץ לכל הגולשים בו, המעוניינים לשתף ולהדליף מידע, להשתמש ברשת האפלה. המעוניינים בכך מופנים לרשת האפלה, ממלאים את פרטי הידיעה ונדרשים לתאר אותה בצורה המפורטת ביותר, ובנוסף לכך להעלות קבצים, כגון תמונות או מסמכים, אשר יוכיחו את אמיתותה, וזאת למרות שאין כל חובה מצד האתר לעשות כן.[40]

פלטפורמת הדלפה עיתונאית נוספת היא מערכת Secure Drop, אשר פותחה וקודמה על ידי הארגון Freedom of the Press Foundation. המערכת מספקת שירותי תקשורת והעברת נתונים בצורה מוצפנת ואנונימית. סינדיקטי עיתונות כגון: "Associated Press", "The Guardian", "The New York Times", "Al Jazeera", וכן גורמים רבים אחרים, משתמשים במערכת זו כדי לחלוק ולקבל מידע רגיש.

ממשלות יכולות לעשות שימוש בשתי הפלטפורמות שהוזכרו לעיל כדי להדליף מידע שפרסומו בתקשורת המסורתית הגלויה עשוי להיות בעייתי מבחינתן. דוגמה מובהקת לכך הוא המידע בדבר הימצאותו של נשק גרעיני ברשות מדינת ישראל:

---

37 Scott Shane, "The Age of Big Leaks", *The New York Times*, February 2, 2019.

38 Chris Bing, "How the FBI Relies on Dark Web Intel Firms as Frontline Investigators", *Cyber Scoop*, April 13, 2017.

39 Topor, "Deep and Dark Webs – Liberty or Abuse".

40 David Leigh, Luke Harding and Charles Arthur, *Wikileaks: Inside Julian Assange's War on Secrecy* (New York: Public Affairs, 2011).

ישראל אינה חתומה על האמנה הבין־לאומית למניעת הפצת נשק גרעיני (NPT), ועל כן פרסום גלוי בדבר הימצאותו של נשק כזה ברשותה עשוי להיות בעייתי מבחינת החוק הבין־לאומי. יחד עם זאת, פרסום יזום של ידיעות על נשק אסטרטגי בצורה אנונימית דווקא, יכול לחזק את מעמדה הגיאו־פוליטי של ישראל ולהוות איתות למדינות עוינות. כך, למשל, ניתן למצוא בעמוד ייעודי מפורסם באתר The Hidden Wiki מידע על תוכנית הגרעין הישראלית, הכולל, בין היתר, את ציר הזמן של התוכנית ואת הדוקטרינה, המדיניות והשיטות ליישומה. מידע נוסף על הגרעין הישראלי, וכן על הגרעין ההודי ופרויקטים אחרים השנויים במחלוקת, נמצא בפורומים נוספים ברשת האפלה.

פלטפורמות פסיביות שייעודן אחסון מידע

מדובר באתרי אחסון או בפורומים שבהם דנים בנושא מסוים וחולקים מידע לגביו. למשל, באתר DOXBIN ברשת האפלה ניתן להעלות מידע וקבצים שהמדליפים מעוניינים לשמור לשעת הצורך או להדליף לכל. דוגמה לכך הוא מידע שהודלף ב־30 במאי 2019 על שלושים עובדי הבולשת הפדרלית של ארצות הברית (FBI), הכולל את כתובותיהם האישיות ודרכי התקשרות אליהם, כולל מספרי טלפון וכתובות דואר אלקטרוני, פירוט על בני משפחותיהם ועוד.

פלטפורמה נוספת לאחסון מידע עליו ניתן לדון גם עם אחרים הם פורומים, כגון פורום בשם IntelExchange, בו חולקים ידיעות (חלקן הקטן מודלף), או פורום בשם The Stock Insider, בו משתמשים שעברו אשרור חולקים מידע על מסחר בבורסות השונות ומדליפים ספקולציות. דרך נוספת לשימוש באתרי אחסון מידע אופיינית לא רק למדליפים זדוניים, אלא גם לגופים ממשלתיים או לאנשי מודיעין, המעוניינים להעביר מידע בצורה אנונימית. אלה "מדביקים" באתרי האחסון קבצים אותם הם רוצים לחלוק עם אחרים, עושים זאת תחת כינוי מטעה ושולחים מסר בתקשורת המסורתית (למשל, בהודעת טקסט) עם אותו כינוי ספציפי.

פלטפורמת סחר

אתרים אנונימיים שלמים מציעים למכור או לקנות מידע מסווג. חברות עיסקיות בעלות אמצעים מעלות פעמים רבות בקשות לקנות הדלפות הנוגעות לפרויקטים של חברות אחרות, ויש מקרים שבהם עיתונאים או אנשי ביון מבקשים לסחור במידע. כך, למשל, באתר SellFile מציעים לסחור במידע ובשירותים באמצעות תשלום במטבע הביטקוין. כשמדובר במִבצעי השפעה, ניתן לרכוש ברשת האפלה מאגרי בוחרים שלמים, הכוללים פרטי התקשרות, כמו גם נטיות פוליטיות. מידע כזה יכול לשמש כדי לסמן מצביעים פוטנציאליים ברשתות החברתיות.

לא רק מידע נסחר בפלטפורמות אלו. לאחרונה פורסם מחקר, לפיו הרשת האפלה הופכת למקור העיקרי למכירה ולמשלוח של נוזקות המותאמות אישית לפריצות

לארגונים ולמגזרי תעשייה ספציפיים.[41] נוזקות אלו עשויות להיות מופעלות גם במסגרת תקיפות סייבר שמטרתן היא שיבוש מערכות בחירות. בכירים בשירותי המודיעין של ארצות הברית מעריכים שקיים סיכוי גבוה כי האקרים ינסו להטות, ואף להשמיד, את מאגרי רישום הבוחרים לקראת בחירות 2020 לנשיאות ארצות הברית באמצעות וירוס כופר (Ransomware). מתקפות סייבר מסוג זה בדרך כלל נועלות מחשבים הנגועים בווירוס עד אשר התשלום, שלרוב מתבצע באמצעות מטבע הקריפטו, נשלח להאקרים. דוגמה לכך היא מתקפת הסייבר העולמית NotPetya שהוצאה לפועל ביוני 2017 ויוחסה לרוסיה. במתקפה זו נעשה שימוש בווירוס כופר לצורך מיסוך טכניקת מחיקת נתונים, מה שהפך את מחשבי הקורבנות לבלתי שמישים לחלוטין. איום זה מדאיג במיוחד לנוכח השפעתו הפוטנציאלית על תוצאות ההצבעה. מתקפה מסוג זה, שלא זוהתה לפני הבחירות, עשויה לחבל ברשימות הבוחרים, ליצור בלבול ועיכובים עצומים, לגרום לשלילת זכות הצבעה, ואף לפגוע משמעותית בתקפותן של תוצאות הבחירות.[42]

כלי נשק דיגיטליים, כמו התוכנות הזדוניות לפריצה EternalBlue ו־WannaCry, שעקבותיהן מוליכות לצפון קוריאה ואשר גרמו בשנת 2018 נזק שנאמד בכמעט ארבעה מיליארד דולר למערכות מחשבים עיסקיים וממשלתיים במספר מדינות, זמינים אף הם ברשת האפלה בעלות נמוכה יחסית. כלים אלה עשויים לשמש גורמים עוינים למבצעי השפעה בסייבר.[43]

מלבד נוזקות וכלי פריצה, לאחרונה ניכר כי פלטפורמות מדיה חברתית עם מספר רב של חשבונות נטושים מהוות מטרה מרכזית ונוחה להאקרים בשל פגיעויות האבטחה הרבות בהן. רשתות בוטים ב"טוויטר", "פייסבוק" ו"אינסטגרם", שמטרתן להפיץ דיסאינפורמציה ולהגדיל את מידת ה"מעורבות", דהיינו Like ו־Share, כדי ליצור מצג שווא של עניין ציבורי סביב תכנים מסוימים, מוצעות למכירה ברשת האפלה תמורת סכומים זעומים. באופן דומה מוצעות למכירה חבילות נפרדות של "ריטוויטים", "לייקים" וצפיות ב"יוטיוב".[44]

לשלוש הפלטפורמות שנסקרו יש שלושה שימושים נפוצים: העצמת המדינה המדליפה; פגיעה במדינה שעליה מדליפים; קידום זכויות האדם במדינה שעליה מדליפים. כך, למשל, באתר РосПравосудие ברשת האפלה פורסמו כחמישים

41 יוסי הטוני, "מהם כלי הפריצה הפופולריים שמוצעים למכירה בדארקנט?", **אנשים ומחשבים**, 11 ביוני 2019.

42 Christopher Bing, "Exclusive: U.S. Officials Fear Ransomware Attack against 2020 Election", *Reuters,* 26 August 2019.

43 Ibid.

44 Dan Patterson, "The Dark Web is Where Hackers Buy the Tools to Subvert Elections", *CBS News,* September 26, 2018; "Influence for Sale: Bot Shopping on the Darknet", *DFRLab*, June 19, 2017.

מיליון מסמכים העוסקים במערכת המשפט הרוסית, שכללו מידע אישי על שופטים, עורכי דין, אנשי פרקליטות ועוד. האתר עצמו מציין כי מפעיליו רוצים להדליף פרטי מידע כדי לגרום לאי־נוחות וללחץ על אלה אשר משתמשים בחוק בצורה מניפולטיבית לטובת הממשל, וחשוב מכך – לרעת אלה העומדים בפני משפט לא הוגן שתוצאותיו כבר נכתבו מראש. לפי שעה לא ברור מי עומד מאחורי אתר זה – אלה המנסים לערער את מעמדה של רוסיה מבפנים ומבחוץ, או אזרחים רוסים המבינים את החשיבות של מערכת משפט תקינה.[45]

להלן מספר דוגמאות לשימושים שכבר נעשו ברשת האפלה בהקשר של השפעה על בחירות: ב־2016 נפרצו השרתים של הוועדה הפדרלית לבחירות בארצות הברית (U.S. Election Assistance Commission), ואישורי כניסה גנובים של עובדיה התגלו ברשת האפלה;[46] באותה שנה השקיעו האקרים רוסיים כ־95,000 דולר במטבע הקריפטו כדי להקים אתרים וחשבונות מדיה חברתית מזויפים ברשת האפלה במטרה להשתמש בהם למִבצעי השפעה;[47] בראשית 2017 חשף משרד המשפטים האמריקאי כי במסגרת מבצעי ההשפעה הרוסיים בבחירות 2016 לנשיאות ארצות הברית, הצליחו האקרים רוסיים להשיג גישה ליותר מחצי מיליארד חשבונות מייל באתר האינטרנט "יאהו". ההאקרים גם הצליחו לחדור לחשבונותיהם של 6,500 משתמשים, וביניהם יעדים שסומנו מראש על ידי הממשל הרוסי, כמו עיתונאים וחברי אופוזיציה. גישה לחשבונות נוספים נמכרה לכל המרבה במחיר ברשת האפלה, ככל הנראה כדי להגדיל את הרווח מהפריצה;[48] ב־2017 גם הוצעו למכירה ברשת האפלה כארבעים מיליון רשומות של אזרחים אמריקאים תמורת ארבעה דולר בלבד. הסכום הנמוך שנדרש תמורת המידע מחזק את הסברה שלא הייתה מטרת רווח מאחורי המכירה, אלא מטרה אידיאולוגית. זאת ועוד, על רקע בחירות אמצע הכהונה בארצות הברית בשלהי 2018, נחשף מאגר מידע של עשרות מיליוני בוחרים אמריקאים שהוצע למכירה ברשת האפלה. המאגר הציע, מלבד פרטיהם האישיים של הבוחרים, גם מידע על השקפותיו הפוליטיות של כל אחד מהם, ובכלל זה האם הוא תומך במועמד רפובליקני או דמוקרטי.[49]

מאגרי מידע אלה יכולים לשמש הן להגברת היעילות בסימון קהלי יעד פוטנציאליים כמטרות והן להגברת תדירותן של מתקפות דיוג. מדובר בהקשר זה

45 Topor, "Deep and Dark Webs – Liberty or Abuse".

46 Menn Joseph, "U.S. Election Agancy Breached by Hackers after November Vote", *Reuters*, December 16, 2016.

47 Topor, "Deep and Dark Webs – Liberty or Abuse".

48 אילן גלר, "פשוט וגאוני: ככה האקרים רוסים פרצו למיליוני חשבונות דואר בלי סיסמה", **וואלה**, 19 במארס 2017.

49 רפאלה גויכמן, "פרטיהם של 62 מיליון בוחרים אמריקאים מוצעים למכירה בדארקנט", **דה מרקר**, 6 בנובמבר 2018.

בהתחזות לספקיות שירות, כמו בנק, מערכת הפעלה או מוסד ממשלתי, במטרה לקבל פרטים אישיים מהמשתמשים, ובאמצעותם להוציא לפועל מבצעי השפעה.[50]

על רקע הבחירות בישראל ב־2019 הוצעו למכירה ברשת האפלה כלי סייבר התקפיים שפותחו על ידי האקרים, ככל הנראה ממוצא אוקראיני, שנועדו להתגבר על ההגבלות שהטילה "ווטסאפ" על מספר אנשי הקשר אליהם ניתן להעביר מסרים בעת ובעונה אחת. כלי הסייבר שהוצעו ברשת מקנים למי שרוכש אותם יכולת להשתלט מרחוק על כל קבוצות ה"ווטסאפ" בישראל ולשתול בתוכן סרטונים או מסרונים כרצונו. מעבר לכך, החברים בקבוצת הצ'ט לא יקבלו את הסרטון ממספר לא מוכר, אלא מאחד החברים האחרים בצ'ט, מה שיגביר את רמת המהימנות של הסרטון.[51] לטענת בן כספית, לאחרונה רכשו גורמים ישראליים במאות אלפי דולרים את האופציה לשיגור 15 מיליון הודעות "ווטסאפ" בתוך 48 שעות. האפשרות של "פייסבוק" לחסום יכולת זאת הינה מוגבלת, אם כי ברשת האפלה יש האקרים המוכרים יכולת הגנת נגד, שתוקפת את הסרטונים הללו עם הופעתם, יוצרת ביקוש מלאכותי עצום וגורמת לקריסת המערכת.[52]

סיכום

מטרתו של מאמר זה היא להסב את תשומת הלב לרשת האפלה כערוץ נוסף להוצאתן לפועל של מתקפות סייבר ומבצעי השפעה בסייבר, ולהסביר כיצד השחקנים השונים מממשים זאת. חשיבותה של הרשת האפלה כפלטפורמה לניסיונות השפעה על מערכות בחירות הולכת וגוברת בחודשים האחרונים, בד בבד עם הִתרבות הניסיונות להתערבות זרה במערכות בחירות ברחבי העולם, בעיקר מצד רוסיה. כפועל יוצא מתופעה זו חלה עלייה במאמצי ההתגוננות של ענקיות המדיה והמדינות עצמן נגד שיטות הפעולה המוכרות בתחום זה. על רקע זה ניכרות ירידה בשימוש בבוטים ברשתות החברתיות לצורך מבצעי השפעה ועלייה בפעילות באפליקציות להעברת מסרים מיידיים. עלייה בפעילות חלה גם ברשת האפלה, המאפשרת פרטיות ואנונימיות במידה גבוהה יותר מאשר ברשת הרגילה, ומשום כך מהווה אתגר להתמודדות עם מבצעי השפעה. מעבר להיותו אתגר טכנולוגי, מדובר גם במקרה זה בהתנגשות בין הצורך להגן על השיח הציבורי ובין עקרון השמירה על חופש הביטוי, אותו חותרת, בין היתר, לקדם הרשת האפלה.

בהמשך המאמר נסקרו שלוש פלטפורמות הדלפה עיקריות ברשת האפלה: פלטפורמות הקוראות למדליפים להדליף מידע, כגון WikiLeaks או Secure Drop;

---

50 Patterson, "The Dark Web is Where Hackers Buy the Tools to Subvert Elections".

51 בן כספית, "האיום על הבחירות הגוריליות האלו נמצא בעולם התחתון של האינטרנט", **מעריב**, 9 בספטמבר 2019.

52 שם.

פלטפורמות פסיביות, כגון DOXBIN, IntelExchange או The Stock Insider, המשמשות לאחסון מידע מודלף; פלטפורמות סחר, דוגמת SellFile, בה מוצע מידע למכירה ומתקבלות בקשות למידע לפי הזמנה. בנוסף לכך, ברשת האפלה זמינים לרכישה נוזקות, רוגלות, רשתות בוטים וכלי סייבר והצפנת תקשורת, באמצעותם ניתן להוציא לפועל את מבצעי ההשפעה בצורה קלה ואנונימית.

כלים אלה, כמו גם שלוש הפלטפורמות המוזכרות לעיל, עשויים לשמש מדינות וארגונים כדי להוציא לפועל מבצעי השפעה במרחב הקיברנטי, כפי שהודגם במאמר. אמנם, מהימנותו של המידע הזורם ברשת האפלה שנויה במחלוקת, אך נראה שפעמים רבות אין הדבר רלוונטי עבור גורמים החותרים להוציא לפועל מבצעי השפעה, שעצם ההדלפה משמשת את מטרתם המרכזית – זריעת ספק וערעור הַסדר הקיים. לנוכח עלותן הנמוכה יחסית של היכולות המוצעות למכירה ברשת האפלה והקושי להתחקות אחר המקורות המדליפים בה, ניתן לצפות בשנים הקרובות לעלייה בהיצע ובביקוש של אמצעים ברשת זו לצורך הוצאתם לפועל של מִבצעי השפעה.

סוגיה מעניינת נוספת העולה מן העיסוק בנושא היא נוכחותם של משטרים דמוקרטיים ברשת האפלה והשימוש שהם עושים בה: מצד אחד, הצורך להתמודד עם חתרנותם של ארגוני טרור ומשטרים טוטליטאריים, כמו גם עם פשיעה, יוצר מצב שבו אין מנוס ממעורבות ברשת האפלה, בבחינת "דע את האויב"; מצד שני, עצם השימוש שעושים משטרים דמוקרטיים ברשת האפלה ובאנונימיות שלה מעורר לכאורה בעייתיות; אמנם, משטרים דמוקרטיים אינם פטורים ממשחק קשוח בזירה הבין־לאומית, אך הדרך בה הם עושים זאת היא בעלת חשיבות, במיוחד כאשר משטרים אלה מתיימרים להיות "ערכיים" יותר מהמשטרים הטוטליטאריים. יש להניח שהמשטר הדמוקרטי שהשיק רשת אפלה גם עושה את השימוש הנרחב ביותר בה, כפי שרמז בכיר בממשל האמריקאי.[53]

שאלה ערכית חשובה נוספת העולה מהמאמר היא: האם משטרים דמוקרטיים עושים שימוש ברשת האפלה לא רק נגד יריבים בזירה הבין־לאומית, אלא גם נגד יריבים מבית? חברי פרלמנט רבים ברחבי העולם, כמו גם חברי כנסת בישראל, מדליפים מידע מישיבות, ואלה הנתפסים עשויים לעמוד לדין. לעומת זאת, הדלפה ברשת האפלה יכולה לאפשר גם אנונימיות גדולה יותר וגם לזרוע כאוס במערכת הפוליטית.

53 לאחד מכותבי המאמר במהלך כנס בוושינגטון בספטמבר 2019.